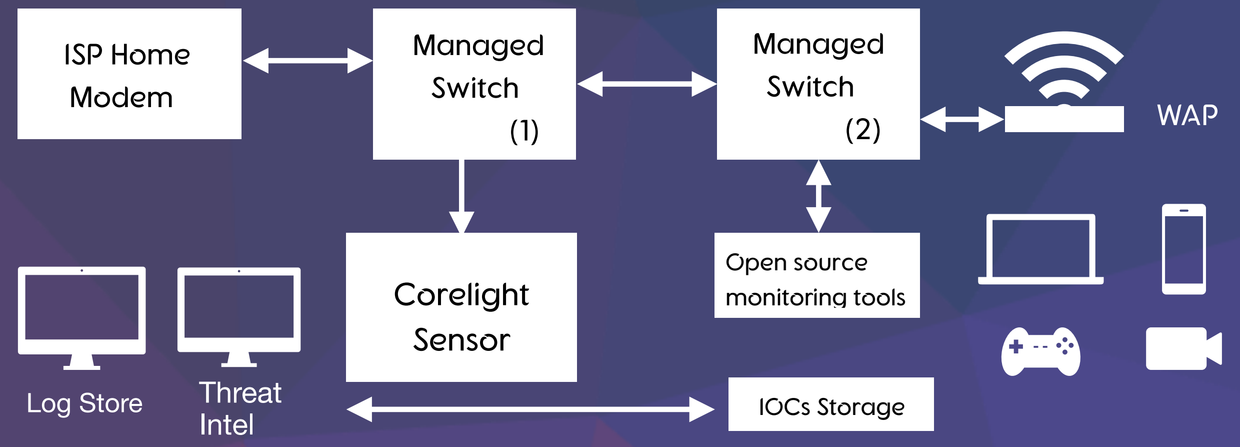
Sheet summary

This sheet will help you install a network monitoring software sensor in a home network and it will use to monitoring all network traffic and malicious activities or insider threats. This sheet is a part of my academic research project about Data Intelligence and building in-house Data Intelligence centre. All tools are open source and free to use after signing agreements or signing up with providers.

You will need a permission to collect logs and data from your home network by your family members. All information shared here is publicly free for research and development and all copy rights reserved to researcher*, software and hardware providers.

Architecture

This architecture represents a small home network and you can extend it with more open source tools or using personal scripts. Corelight sensor connected to managed switch (1) to monitoring ingress and egress network traffic with Threat Intelligence capabilities.



ISP Home Modem

Managed Switch (1)

Managed Switch (2)

WAP

Corelight Sensor

Open source monitoring tools

IOCs Storage

Log Store

Threat Intel

Requirements

1. Raspberry Pi v4 (Includes: SD Card, Power Supply, HDMI Cable, Keyboard, Mouse)
2. Corelight Software Agreement (Free)
3. Managed Switch (Any type)
4. Humio free cloud account (Community Edition)

Notes

- Preferred to purchase Raspberry PI CanaKit V4 (Recommend 8 GB RAM).
- You can add more software sensors to your home network (e.g. connect to managed switch (2) [Mirror Port] to detect lateral movement inside home network).
- Corelight software sensor combines Zeek and Suricata, recommend to download Bro cheatsheets from Corelight Resources section in this sheet.
- Corelight software sensor supports stream exporters (e.g. Splunk) via HTTP Event collector.

Data Intelligence

All software rights reserved to corelight and humio

corelight

humio
A CrowdStrike Company

All hardware rights reserved to Raspberry PI

Raspberry Pi

* All sheet rights reserved to Data Intelligence research project and researcher (Amgad.M)

Configuration steps

Installation:

1. Open a terminal on Raspberry PI
2. Install raspi-corelight from Github by executing the following command:
   `source <( curl https://raw.githubusercontent.com/corelight/raspi-corelight/main/raspi-corelight)`
3. Execute the script by using the following command: raspi-corelight
4. After rebooting, run the script (raspi-corelight) and use idaptive username and password.

Note: You will get idaptive username after accepting a corelight agreement.

5. Use qc command for a quick config then adding the following information:
   - Add monitoring interface
   - Validate licence
   - Add Humio API token

Optional: you can configure Splunk exporter.

6. Reboot Raspberry PI

Edit Configuration File:

File Path: /etc/corelight-softsensor.conf

Optional: GeoIP isn't available and you can configure an external database (e.g. Maxmind)

Note: you can enable Suricata from configuration file: corelight-softsensor.conf

Recommend: Install Suricata-update tool, to manage Suricata rulesets.

Note: customize Suricata rules is limited and enabling Suricata effects performance.

Dashboard Configuration: (From corelight-softsensor.conf file)

Corelight software sensor supports Grafana dashboard and querying Prometheus.

Resources

Corelight:

https://corelight.com/blog/2020/04/08/enabling-soho-network-security-monitoring
https://corelight.com/blog/2020/11/19/corelight-at-home
https://go.corelight.com/corelight-at-home
https://www.youtube.com/watch?v=2bNmg1n6wTA
https://github.com/corelight/raspi-corelight
https://github.com/corelight/bro-cheatsheets

Humio:

https://www.humio.com/whats-new/blog/monitor-home-network-with-corelight-humio/

Raspberry PI:

https://www.canakit.com/raspberry-pi-4-starter-kit.html
https://www.raspberrypi.com/software/

Incident Response Book:

https://www.appliedincidentresponse.com/

Threat Intelligence Tools/Framework:

https://www.opencti.io/en/
https://www.misp-project.org/
https://docs.zeek.org/en/current/frameworks/intel.html